**Unit 3 Lab: Identifying and Removing Malware on a Windows System**

Desmond Hughes

Purdue University Global

IT262 Certified Ethical Hacking I

Cheryl Waters

July 25, 2022

Section 1: The first High Severity threat is Win32:Malware-gen (C:\Helix\IR\bin\cryptcat.exe)

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, application

Description automatically generated

Section 2: The Last High Severity Threat is Win32:BO-G[Trj] (in C:\Users\Administrator\AppData\Local\1\BO\BOG

Graphical user interface, text, application

Description automatically generated

Graphical user interface, website

Description automatically generated

Graphical user interface, text, application

Description automatically generatedA screenshot of a computer

Description automatically generatedGraphical user interface, application

Description automatically generated

Section 3 Part 1: WinNuke was made in 1997, and was used to attack Windows 95 and Windows NT. There was also a version that targeted Windows 2000, and Windows XP. WinNuke was used to mess up network communications by disabling it and disturbing it. To get the network communication to work again you would have to restore the system. To stop the attack from happening you would have to get a patch. I think WinNuke is still dangerous, because a newer version could be created, and start to attack users, and will require them to download an oath or it may even lead to more serious consequences.

Part 2: McAfree is good for beginnings, and it is intuitive and inexpensive. It is also great for internet security. TotalAV is a very strong and protect antivirus software. It keeps your computer safe from new and even advance threats. “It offers robust protection against viruses, trojans, ransomware, phishing scams, and malware.” ("Best Antivirus Software for the USA - Jul 2022 - Cybernews.com", 2022). Bitdefender has all the security essentials, and has good security for the internet. It also has features like Parental Control and File Backup. It is also best in malware detection with solid tracking protection. The one I will most likely pick is TotalAV it is the number one recommended, and has a strong protect against attacks. TotalAV fights against new and stronger threats.

Step 2: Antivirus software should detect a wide range of viruses, like all existing malware, worms and trojan viruses. There are different ways antivirus software can identify malware. Methods like anti-malware signature, heuristic analysis, and behavioral audits. Anti-malware signature is the most common used way to identify and fight against malware. It uses signatures that uses files or codes that have been discovered as a problem.

Heuristic analysis analyzes the code and how It is written, and when it is analyzed, it is determined if it is a problem or not, or when it is analyzed, it determines the code’s purpose and why it is used. It determines the purpose by using common indicators, and when it done it comes to that conclusion. But Heuristic analysis can also lead to false conclusions. With it sometimes having false conclusions it is often paired up with another method, so that the identification is correct. Behavioral Audits of malware executes a code and when that code is executed it is observed by the interactions it makes, By the interactions it makes Behavioral Audits of Malware finds out the code’s intent. The audits are performed by a user. The environment they are set in is usually virtual or sandboxed, to not cause harm that the malware can cause while seeing the effects of the code while it is being ran and audited. These methods are sometimes combined to understand and discover the malware, so that they know the best way to protect against the attacks.

Reference

Best Antivirus Software for the USA - Jul 2022 - Cybernews.com. (2022). Retrieved 25 July 2022, from https://us.cybernews.com/lp/best-antivirus-software-us/?campaignId=15433224879&adgroupId=133072260673&adId=581044162791&targetId=kwd-548715275&device=c&gunique=Cj0KCQjw\_viWBhD8ARIsAH1mCd5vorGCvYA4lOKFhlkD3a0luCg59ScFe5bvJ044KNr5c\_Z1OZcuKNYaAoo\_EALw\_wcB&gclid=Cj0KCQjw\_viWBhD8ARIsAH1mCd5vorGCvYA4lOKFhlkD3a0luCg59ScFe5bvJ044KNr5c\_Z1OZcuKNYaAoo\_EALw\_wcB

Limited, S. (2022). Malware Identification: The Evolution of Malware. Retrieved 26 July 2022, from https://www.sitelock.com/blog/evolution-of-malware-identification/

WinNuke lives on, and it's coming to a system near you. (2002). Retrieved 25 July 2022, from https://www.techrepublic.com/article/winnuke-lives-on-and-its-coming-to-a-system-near-you/